Information Technology Security Audit

Audit Categories

Criminal Justice Audit – an audit of a criminal justice agency's access, use, storage, and destruction of any Criminal Justice Information (CJI) received from FBI Criminal Justice Information Services (CJIS) Division systems for criminal justice purposes via both direct and indirect access methods. These audits include both name-based and fingerprint-based queries over wired or wireless networks.

Non-criminal Justice Audit – an audit of a non-criminal justice agency's access, use, storage, and destruction of any CJI received from FBI CJIS systems for non-criminal justice purposes via direct and indirect access methods. These audits include both name-based and fingerprint-based queries over wired or wireless networks.

Outsourcing/Channeling Audit – an audit of an FBI approved contractor who submits fingerprints on behalf of an authorized recipient to the FBI and receives the results of such a submission for dissemination back to the authorized recipient. The scope of channeler audits focuses mainly on the storage, dissemination, and destruction of criminal history record information (CHRI).

These audits are comprised of an administrative interview to review administrative and technical controls implemented to protect CJI from both a physical and logical perspective. Additionally, most audits include a physical security and network inspection in which controls identified in the administrative interview are verified to be implemented and working correctly.

Audit Objective(s)/Scope

The purpose of the audit is to assess the user community's compliance with the FBI *CJIS Security Policy* requirements as approved by the Advisory Policy Board (APB) and National Crime Prevention and Privacy Compact (Compact) Council. The FBI *CJIS Security Policy* provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives.

The FBI *CJIS Security Policy* applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The FBI *CJIS Security Policy* provides the minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, and/or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for non-criminal justice purposes are also governed by the standards and rules promulgated by the Compact Council to include the Outsourcing Standard for Channelers.

Overview of the Process

Pre-audit

Prior to the on-site audits, the CJIS Audit Unit (CAU) auditors contact the CJIS Systems Officer (CSO) or Information Security Officer (ISO) and local agency representatives to schedule the audit date and to give an overview of the audit process. They also gather basic audit information and discuss pre-audit responsibilities.

The CSA pre-audit questionnaire is used to assist the audit manager in gathering pertinent information prior to the on-site visit. Information gathered from the pre-audit questionnaire is used to formulate additional questions to be answered during the on-site visit and to assist in determining policy compliance. Additionally, the pre-audit questionnaire is used as a tool by audit managers to prepare information sheets for local auditors, outlining/summarizing the CSA's audit program and procedures.

Information that is requested in the pre-audit questionnaire includes:

- Agreements utilized at the CSA and/or local agencies (e.g., management control agreements, CJIS Security Addendums).
- Policies and procedures utilized at the CSA and/or local agencies (e.g., personnel sanctions, physical and electronic media protection, security incident response, etc.).
- Security Awareness Training materials and records.
- Current technical security audit report for each of the agencies selected for the audit.
- Background of network infrastructure which identifies all networks and information systems utilized to store, access, or transmit CJI for criminal or non-criminal justice purposes.
- Description of measures taken to protect those identified networks and information systems (boundary protection, encryption, authentication, account management, system event logs, etc.).

The local pre-audit packet is used to assist local auditors in determining the agency's compliance with FBI *CJIS Security Policy* policies and procedures. This information is mailed prior to the audit and reviewed during the on-site visit.

Agency Selection

The Information Technology Security (ITS) Audit program is designed to assess agency compliance with the FBI *CJIS Security Policy*. This is accomplished through a review of administrative policies and procedures, as well as on-site network inspections, at the CSA and a sample of local agencies (usually 10-16) within the jurisdiction of the CSA. The ITS Audit program's local agency selection process is limited to a variety of constraints to include: logistics, geography, fiscal and personnel resource limitations, and CSO/ISO input.

Assessment

During the CSA visit, the audit manager interviews the CSO/ISO and CSA personnel to determine the CSA's adherence to FBI *CJIS Security Policy* policies and procedures.

During local audits, auditors conduct interviews with local agency representatives to determine the agency's adherence to FBI *CJIS Security Policy* policies and procedures. Additionally, an on-site network inspection is conducted. Upon completion of the on-site interviews and network inspections, auditors determine compliance with FBI *CJIS Security Policy* policies and procedures.

After all interviews and network inspection assessments are completed, exit interviews with the CSO/ISO and local agency representatives are conducted to inform them of compliance issues and copies of the results are disseminated.

Post-audit

Upon completion of the audit, the CAU will provide the results and recommendations from the audit to the CSO. The CAU will also provide policy/reference material and additional supporting audit documentation, if appropriate. The CSO is requested to review the findings and to respond to recommendations, if any, by indicating corrective actions that will be taken. The CAU will provide the audit results, including the CSO's response to the required actions, to the CJIS Advisory Policy Board's Compliance Evaluation Subcommittee (CES) for criminal justice audits or the National Crime Preventions and Privacy Compact Council's Sanctions Committee for non-criminal justice and channeler audits, for review and appropriate action.